

09/403071  
日 本 国 特 許 庁 08.02.99  
PATENT OFFICE  
JAPANESE GOVERNMENT

E.U.

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office.

出 願 年 月 日  
Date of Application:

1998年 2月13日

REC'D 26 MAR 1999

WIPO PCT

出 願 番 号  
Application Number:

平成10年特許願第031847号

出 願 人  
Applicant(s):

松下電器産業株式会社

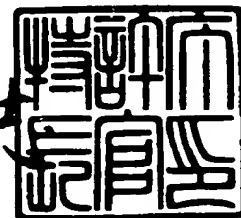
**PRIORITY  
DOCUMENT**

SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH RULE 17.1(a) OR (b)

1999年 3月12日

特許庁長官  
Commissioner,  
Patent Office

伴佐山 建志



出証番号 出証特平11-3013025

【書類名】	特許願
【整理番号】	2054001030
【提出日】	平成10年 2月13日
【あて先】	特許庁長官殿
<hr/>	
【国際特許分類】	H04L 9/00
【発明の名称】	デジタルAVデータ送信ユニット、デジタルAVデータ 受信ユニット及び、デジタルAVデータ送受信システム 、媒体
【請求項の数】	17
【発明者】	
【住所又は居所】	大阪府門真市大字門真1006番地 松下電器産業株式 会社内
【氏名】	飯塚 裕之
【発明者】	
【住所又は居所】	大阪府門真市大字門真1006番地 松下電器産業株式 会社内
【氏名】	山田 正純
【発明者】	
【住所又は居所】	大阪府門真市大字門真1006番地 松下電器産業株式 会社内
【氏名】	武知 秀明
【発明者】	
【住所又は居所】	大阪府門真市大字門真1006番地 松下電器産業株式 会社内
【氏名】	臼木 直司
【発明者】	
【住所又は居所】	大阪府門真市大字門真1006番地 松下電器産業株式 会社内
【氏名】	後藤 昌一

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100092794

【弁理士】

【氏名又は名称】 松田 正道

【電話番号】 06 397-2840

【手数料の表示】

【予納台帳番号】 009896

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9006027

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 デジタルAVデータ送信ユニット、デジタルAVデータ受信ユニット及び、デジタルAVデータ送受信システム、媒体

【特許請求の範囲】

【請求項1】 デジタルAVデータの重要度を判定するデータ重要性判定手段と、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証要求を受け、前記データ重要性判定手段の判定結果に基づき、前記送信側複数認証ルール格納手段から一種類のルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも備えたことを特徴とするデジタルAVデータ送信ユニット。

【請求項2】 デジタルAVデータの重要度を判定するデータ重要性判定手段と、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証要求を受け、前記データ重要性判定手段の判定結果に基づき、前記送信側複数認証ルール格納手段から一種類のルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも有するデジタルAVデータ送信ユニットを通信の対象とし、

前記認証の要求を行う認証要求手段と、前記送信側複数認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、前記送信側認証選択手段で選択された所定の認証ルールと同じ認証ルールを前記受信側複数認証ルール格納手段から選択する受信側認証選択手段と、受信側で前記選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも備えたことを特徴とするデジタルAVデータ受信ユニット。

【請求項3】 デジタルAVデータの重要度を判定するデータ重要性判定手段と、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証要求を受け、前記データ重要性判定手段の判定結果に基づき、前記送信側複数認証ルール格納手段から一種類のルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも有するデジタルAV送信ユニットと、

前記認証の要求を行う認証要求手段と、前記送信側複数認証ルール格納手段と

同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、前記送信側認証選択手段で選択された所定の認証ルールと同じ認証ルールを前記受信側複数認証ルール格納手段から選択する受信側認証選択手段と、受信側で前記選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも有するデジタルAVデータ受信ユニットとを備えたことを特徴とするデジタルAVデータ送受信システム。

【請求項4】 デジタルAVデータの重要度を判定するデータ重要性判定手段と、所定の管理基準を格納した管理基準格納手段と、認証要求を受け、前記データ重要性判定手段の判定結果に基き、前記管理基準格納手段の前記管理基準を参照すべきかどうか決定する管理基準参照決定手段と、その決定された結果に従って前記管理基準を参照してそれに従い認証すべきかどうか、あるいは認証の種類を決定する認証決定手段と、その認証決定手段の決定に従って、所定の認証ルールに基づいて認証を行う認証手段とを少なくとも備えたことを特徴とするデジタルAVデータ送信ユニット。

【請求項5】 前記送信ユニットは前記受信ユニットの各機能を有し、前記受信ユニットは前記送信ユニットの各機能を有することを特徴とする請求項3記載のデジタルAVデータ送受信システム。

【請求項6】 前記受信ユニットの機能を有する送信ユニット、あるいは前記送信ユニットの機能を有する受信ユニットが三つ以上互いに接続され、デジタルAVデータを互いにやりとりできることを特徴とする請求項5記載のデジタルAVデータ送受信システム。

【請求項7】 複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルAVデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記デジタルAVデータ受信ユニットが有する認証ルールを、前記送信側複数認証ルール格納手段から取り出す送信側認証ルール取り出し手段と、それに基づき前記認証を行う送信側認証手段とを少なくとも備えたデジタルAV送信ユニット。

【請求項8】 複数種類の認証ルールを格納した送信側複数認証ルール格納手

段と、デジタルAVデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記デジタルAVデータ受信ユニットが有する認証ルールを、前記送信側複数認証ルール格納手段から取り出す送信側認証ルール取り出し手段と、それに基づき前記認証を行う送信側認証手段とを少なくとも有するデジタルAV送信ユニットを通信の対象とし、

前記認証の要求を行う認証要求手段と、自らの一種類の前記認証ルールを格納する受信側認証ルール格納手段と、前記認証ルールについての情報を送信する認証ルール情報送信手段と、前記送信ユニットとの間で前記認証ルールにて認証を行う受信側認証手段とを少なくとも備えたことを特徴とするデジタルAVデータ受信ユニット。

【請求項9】 複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルAVデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記デジタルAVデータ受信ユニットが有する認証ルールを、前記送信側複数認証ルール格納手段から取り出す送信側認証ルール取り出し手段と、それに基づき前記認証を行う送信側認証手段とを少なくとも有するデジタルAV送信ユニットと、

前記認証の要求を行う認証要求手段と、自らの一種類の前記認証ルールを格納する受信側認証ルール格納手段と、前記認証ルールについての情報を送信する認証ルール情報送信手段と、前記送信ユニットとの間で前記認証ルールにて認証を行う受信側認証手段を少なくとも有するデジタルAVデータ受信ユニットと、を備えたことを特徴とするデジタルAVデータ送受信システム。

【請求項10】 所定の管理基準を格納した管理基準格納手段と、デジタルAVデータ受信ユニットから認証要求を受けて、そのデジタルAVデータ受信ユニットの種類又は重要度に応じて、前記管理基準格納手段の前記管理基準を参照すべきかどうか決定する管理基準参照決定手段と、その決定された結果に従って前記管理基準を参照してそれに従い認証すべきかどうか、あるいは認証の種類を決

定する認証決定手段と、その認証決定手段の決定に従って、所定の認証ルールに基づいて認証を行う認証手段とを少なくとも備えたことを特徴とするデジタルAV送信ユニット。

—【請求項11】 前記管理基準は、不正な、あるいは正当なデジタルAVデータ受信ユニットを識別できる基準リスト（CRL）であることを特徴とする請求項4又は10に記載のデジタルAV送信ユニット。

【請求項12】 前記送信ユニットに、前記受信ユニットが二つ以上接続され、前記送信ユニットとの間で、デジタルAVデータをやりとりできることを特徴とする請求項9記載のデジタルAVデータ送受信システム。

【請求項13】 複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルAVデータの重要度を判定するデータ重要性判定手段と、前記データ重要性判定手段の判定結果に基づき、前記送信側複数認証ルール格納手段から一種類の認証ルールを選択する送信側認証選択手段と、単一認証デジタルAVデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記単一認証デジタルAVデータ受信ユニットが有する認証ルールを、前記送信側複数認証ルール格納手段から取り出す送信側認証取り出し手段と、前記送信側認証選択手段又は前記送信側認証取り出し手段から得られた認証ルールに基づき認証を行う送信側認証手段とを少なくとも備えたことを特徴とするデジタルAVデータ送信ユニット。

【請求項14】 複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルAVデータの重要度を判定するデータ重要性判定手段と、前記データ重要性判定手段の判定結果に基づき、前記送信側複数認証ルール格納手段から一種類の認証ルールを選択する送信側認証選択手段と、単一認証デジタルAVデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記単一認証デジタルAVデータ受信ユニットが有する認証ルールを、前記送信側複数認証ルール格納手段から取り出す送信側認証取り出し手段と、前記送信側認証選択手段又は前記送信側認

証取り出し手段から得られた認証ルールに基づき認証を行う送信側認証手段とを少なくとも有するデジタルAVデータ送信ユニットと、

前記認証の要求を行う認証要求手段と、前記送信側認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、前記送信側認証選択手段で選択された所定の認証ルールと同じ認証ルールを前記受信側複数認証ルール格納手段から選択する受信側認証選択手段と、受信側で前記選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも有する複数認証デジタルAVデータ受信ユニットと、

認証の要求を行う認証要求手段と、自らの一種類の認証ルールを格納する受信側単一認証ルール格納手段と、前記認証ルールについての情報を送信する認証ルール情報送信手段と、前記デジタルAVデータ送信ユニットとの間で前記認証ルールにて認証を行う受信側認証手段を少なくとも有する単一認証デジタルAVデータ受信ユニットと、を備えたことを特徴とするデジタルAVデータ送受信システム。

【請求項15】前記複数認証デジタルAVデータ受信ユニットは前記デジタルAVデータ送信ユニットの各機能を有し、前記デジタルAVデータ送信ユニットは前記複数認証デジタルAVデータ受信ユニットの各機能を有することを特徴とする請求項14記載のデジタルAVデータ送受信システム。

【請求項16】前記複数認証デジタルAVデータ受信ユニットの各機能を有するデジタルAVデータ送信ユニット、あるいは前記デジタルAVデータ送信ユニットの機能を有する複数認証デジタルAVデータ受信ユニットが二つ以上互いに接続され、且つ、前記単一認証デジタルAVデータ受信ユニットが二つ以上接続され、デジタルAVデータを互いにやりとりできることを特徴とする請求項15記載のデジタルAVデータ送受信システム。

【請求項17】請求項1～16のいずれかに記載のユニット又はシステムが有する各構成要素が持つ機能の全部又は一部を実現するためのプログラムを格納したことを特徴とする媒体。

【発明の詳細な説明】

【0001】



## 【発明の属する技術分野】

本発明は、A V装置間において認証を行う機能を持つA Vシステムに関するものである。

---【0002】---

## 【従来の技術】

従来のA V装置間において認証を行うシステムについて図2と図3を用いて説明する。

## 【0003】

まず、図2において、デジタルA Vデータ送信ユニットSTB18は、公開鍵と秘密鍵20、認証手段19、デジタルインターフェースD-I/F22、暗号化手段19を備えている。その公開鍵と秘密鍵20は、認証手段19を介して、デジタルインターフェースD-I/F22に接続している。また、暗号化手段19は、公開鍵と秘密鍵20を参照することが出来、デジタルインターフェース22に接続している。デジタルA Vデータ受信ユニットTV23も公開鍵と秘密鍵26、認証手段25、デジタルインターフェースD-I/F24、復号化手段27を具備している。その公開鍵と秘密鍵26は認証手段25を介してデジタルインターフェースD-I/F24に接続している。また、復号化手段27は公開鍵と秘密鍵26を参照することが出来、デジタルインターフェースD-I/F24に接続している。さらにデジタルインターフェースD-I/F22とデジタルインターフェースD-I/F24は互いにデータのやり取りが出来る構成となっている。

## 【0004】

次にデジタルA Vデータ送信ユニットSTB18とデジタルA Vデータ受信ユニットTV23間の動作を説明する。まず、デジタルA Vデータ受信ユニットTV23が認証要求を出す。するとデジタルインターフェースD-I/F24を通してデジタルA Vデータ送信ユニットSTB18を構成するデジタルインターフェースD-I/F22に認証要求が到達する。デジタルインターフェースD-I/F22は認証要求を受けて認証手段19にて、公開鍵と秘密鍵20を参照して認証する。デジタルA Vデータ送信ユニットSTB18にて認証されれば、暗号

化手段21において、データが暗号化されて、デジタルインターフェースD-I/F22を介して、暗号化したデータが送信される。これはデジタルインターフェースD-I/F24を介して、公開鍵と秘密鍵26を参照して、復号化手段27で復号される。

【0005】

このようにすると、偽造や改竄に強い機能が実現出来る。しかし、公開鍵と秘密鍵を用いた認証は多くの時間を要する。ニュースのように、あまり重要でないデータの場合、不必要に認証に時間を取られることがある。またVTRのようにコピー可能なデータしか受け取っては機器は、場合によってデジタルAVデータ受信ユニットが厳密な認証を要しないこともあり、そのような場合、時間の無駄が生じる。

【0006】

次に、図3において、デジタルAV送信ユニットSTB28は共通鍵30、認証手段29、デジタルインターフェースD-I/F32、暗号化手段31を具備している。その共通鍵30は、認証手段29を介して、デジタルインターフェースD-I/F32に接続している。また、暗号化手段31は、共通鍵30を参照することが出来、デジタルインターフェース32に接続している。デジタルAVデータ受信ユニットTV33も、共通鍵36、認証手段35、デジタルインターフェース34、復号化手段37を具備している。その共通鍵36は認証手段35を介してデジタルインターフェース34に接続している。また、復号化手段37は共通鍵36を参照することが出来、デジタルインターフェース34に接続している。さらにデジタルインターフェース32とデジタルインターフェース34は互いにデータのやり取りが出来る構成となっている。

【0007】

次にデジタルAVデータ送信ユニットSTB28とデジタルAVデータ受信ユニットTV33間の動作を説明する。まず、デジタルAV受信ユニットTV33が認証要求を出す。するとデジタルインターフェースD-I/F34を通してデジタルAV送信ユニットSTB28を構成するデジタルインターフェースD-I/F32に認証要求が到達する。デジタルインターフェースD-I/F32は認

証要求を受けて認証手段 29 にて、共通鍵 30 を参照して認証する。デジタル AV 送信ユニット STB 28 にて認証されれば、暗号化手段 31 において、データが暗号化されて、デジタルインターフェース D-I/F 32 を介して、暗号化したデータが送信される。~~これはデジタルインターフェース D-I/F 34 を介して、~~共通鍵 36 を参照してデジタル復号化手段 37 で復号される。

【0008】

このようにすると、短い時間でデータの認証を行うことができる。しかし、共通鍵を用いた認証は偽造や改竄に弱いので、新作の映画など著作権上重要なデータの場合、第三者にデータを無料で視聴されることがある。また TV のように受信した全てのデータを表示するために、厳密な認証を行う機器と接続した場合に対応できる必要があり、デジタル AV データ受信ユニットが厳密な認証を要する場合があります、そのような場合重要なデータの著作権が保護されないといったことが起こりうる。

【0009】

【発明が解決しようとする課題】

このように、あまり重要でないデータの認証に多くの時間を要するという課題や、重要なデータであるにもかかわらずその認証が偽造や改竄に弱いという課題が存在する。また、デジタル AV データ受信ユニットによっては、厳密な認証を要しないものも存在し、このようなユニットに対して厳密な認証を行った場合、時間の無駄が生じるという課題や、逆にデジタル AV データ受信ユニットによっては厳密な認証を要するものも存在し、そのようなユニットに厳密でない認証を行った場合、著作権が守られないといった課題が存在する。

【0010】

本発明は、このような従来の、重要でないデータの認証に多くの時間を要するという課題と、重要なデータであるにもかかわらずその認証が偽造や改竄に弱いという課題と、ユニットによって認証に必要な厳密さが異なるといった課題を考慮し、データの重要性や相手の装置が有する認証方法の種別などを考慮して、適切な認証方法でデータの送受信を行いうるユニット、システム等を提供することを目的とするものである。

## 【0011】

## 【課題を解決するための手段】

上述した課題を解決するために、請求項1の本発明は、デジタルAVデータの重要度を判定するデータ重要性判定手段と、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証要求を受け、前記データ重要性判定手段の判定結果に基き、前記送信側複数認証ルール格納手段から一種類のルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも備えたことを特徴とするデジタルAVデータ送信ユニットである。

## 【0012】

また請求項2の本発明は、デジタルAVデータの重要度を判定するデータ重要性判定手段と、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証要求を受け、前記データ重要性判定手段の判定結果に基き、前記送信側複数認証ルール格納手段から一種類のルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも有するデジタルAVデータ送信ユニットを通信の対象とし、

前記認証の要求を行う認証要求手段と、前記送信側複数認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、前記送信側認証選択手段で選択された所定の認証ルールと同じ認証ルールを前記受信側複数認証ルール格納手段から選択する受信側認証選択手段と、受信側で前記選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも備えたことを特徴とするデジタルAVデータ受信ユニットである。

## 【0013】

また請求項3の本発明は、デジタルAVデータの重要度を判定するデータ重要性判定手段と、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証要求を受け、前記データ重要性判定手段の判定結果に基き、前記送信側複数認証ルール格納手段から一種類のルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも有するデジタルAV送信ユニットと、

前記認証の要求を行う認証要求手段と、前記送信側複数認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、前記送信側認証選択手段で選択された所定の認証ルールと同じ認証ルールを前記受信側複数認証ルール格納手段から選択する受信側認証選択手段と、受信側で前記選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも有するデジタルAVデータ受信ユニットとを備えたことを特徴とするデジタルAVデータ送受信システムである。

【0014】

また請求項4の本発明は、デジタルAVデータの重要度を判定するデータ重要性判定手段と、所定の管理基準を格納した管理基準格納手段と、認証要求を受け、前記データ重要性判定手段の判定結果に基づき、前記管理基準格納手段の前記管理基準を参照すべきかどうか決定する管理基準参照決定手段と、その決定された結果に従って前記管理基準を参照してそれに従い認証すべきかどうか、あるいは認証の種類を決定する認証決定手段と、その認証決定手段の決定に従って、所定の認証ルールに基づいて認証を行う認証手段とを少なくとも備えたことを特徴とするデジタルAVデータ送信ユニットである。

【0015】

また請求項5の本発明は、前記送信ユニットは前記受信ユニットの各機能を有し、前記受信ユニットは前記送信ユニットの各機能を有することを特徴とする請求項3記載のデジタルAVデータ送受信システムである。

【0016】

また請求項6の本発明は、前記受信ユニットの機能を有する送信ユニット、あるいは前記送信ユニットの機能を有する受信ユニットが三つ以上互いに接続され、デジタルAVデータを互いにやりとりできることを特徴とする請求項5記載のデジタルAVデータ送受信システムである。

【0017】

また請求項7の本発明は、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルAVデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認

証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記デジタルAVデータ受信ユニットが有する認証ルールを、前記送信側複数認証ルール格納手段から取り出す送信側認証ルール取り出し手段と、それに基づき前記認証を行う送信側認証手段とを少なくとも備えたデジタルAV送信ユニットである。

【0018】

また請求項8の本発明は、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルAVデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記デジタルAVデータ受信ユニットが有する認証ルールを、前記送信側複数認証ルール格納手段から取り出す送信側認証ルール取り出し手段と、それに基づき前記認証を行う送信側認証手段とを少なくとも有するデジタルAV送信ユニットを通信の対象とし、

前記認証の要求を行う認証要求手段と、自らの一種類の前記認証ルールを格納する受信側認証ルール格納手段と、前記認証ルールについての情報を送信する認証ルール情報送信手段と、前記送信ユニットとの間で前記認証ルールにて認証を行う受信側認証手段とを少なくとも備えたことを特徴とするデジタルAVデータ受信ユニットである。

【0019】

また請求項9の本発明は、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルAVデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記デジタルAVデータ受信ユニットが有する認証ルールを、前記送信側複数認証ルール格納手段から取り出す送信側認証ルール取り出し手段と、それに基づき前記認証を行う送信側認証手段とを少なくとも有するデジタルAV送信ユニットと

前記認証の要求を行う認証要求手段と、自らの一種類の前記認証ルールを格納

する受信側認証ルール格納手段と、前記認証ルールについての情報を送信する認証ルール情報送信手段と、前記送信ユニットとの間で前記認証ルールにて認証を行う受信側認証手段を少なくとも有するデジタルAVデータ受信ユニットと、を備えたことを特徴とするデジタルA-Vデータ送受信システムである。

## 【0020】

また請求項10の本発明は、所定の管理基準を格納した管理基準格納手段と、デジタルAVデータ受信ユニットから認証要求を受けて、そのデジタルAVデータ受信ユニットの種類又は重要度に応じて、前記管理基準格納手段の前記管理基準を参照すべきかどうか決定する管理基準参照決定手段と、その決定された結果に従って前記管理基準を参照してそれに従い認証すべきかどうか、あるいは認証の種類を決定する認証決定手段と、その認証決定手段の決定に従って、所定の認証ルールに基づいて認証を行う認証手段とを少なくとも備えたことを特徴とするデジタルAV送信ユニットである。

## 【0021】

また請求項11の本発明は、前記管理基準は、不正な、あるいは正当なデジタルAVデータ受信ユニットを識別できる基準リスト(CRL)であることを特徴とする請求項4又は10に記載のデジタルAV送信ユニットである。

## 【0022】

また請求項12の本発明は、前記送信ユニットに、前記受信ユニットが二つ以上接続され、前記送信ユニットとの間で、デジタルAVデータをやりとりできることを特徴とする請求項9記載のデジタルAVデータ送受信システムである。

## 【0023】

また請求項13の本発明は、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルAVデータの重要度を判定するデータ重要性判定手段と、前記データ重要性判定手段の判定結果に基づき、前記送信側複数認証ルール格納手段から一種類の認証ルールを選択する送信側認証選択手段と、単一認証デジタルAVデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記単一認証デジタ

ルAVデータ受信ユニットが有する認証ルールを、前記送信側複数認証ルール格納手段から取り出す送信側認証取り出し手段と、前記送信側認証選択手段又は前記送信側認証取り出し手段から得られた認証ルールに基づき認証を行う送信側認証手段とを少なくとも備えたことを特徴とするデジタルAVデータ送信ユニットである。

【0024】

また請求項14の本発明は、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルAVデータの重要度を判定するデータ重要性判定手段と、前記データ重要性判定手段の判定結果に基づき、前記送信側複数認証ルール格納手段から一種類の認証ルールを選択する送信側認証選択手段と、単一認証デジタルAVデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記単一認証デジタルAVデータ受信ユニットが有する認証ルールを、前記送信側複数認証ルール格納手段から取り出す送信側認証取り出し手段と、前記送信側認証選択手段又は前記送信側認証取り出し手段から得られた認証ルールに基づき認証を行う送信側認証手段とを少なくとも有するデジタルAVデータ送信ユニットと、

前記認証の要求を行う認証要求手段と、前記送信側認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、前記送信側認証選択手段で選択された所定の認証ルールと同じ認証ルールを前記受信側複数認証ルール格納手段から選択する受信側認証選択手段と、受信側で前記選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも有する複数認証デジタルAVデータ受信ユニットと、

認証の要求を行う認証要求手段と、自らの一種類の認証ルールを格納する受信側単一認証ルール格納手段と、前記認証ルールについての情報を送信する認証ルール情報送信手段と、前記デジタルAVデータ送信ユニットとの間で前記認証ルールにて認証を行う受信側認証手段を少なくとも有する単一認証デジタルAVデータ受信ユニットと、を備えたことを特徴とするデジタルAVデータ送受信システムである。



## 【0025】

また請求項15の本発明は、前記複数認証デジタルAVデータ受信ユニットは前記デジタルAVデータ送信ユニットの各機能を有し、前記デジタルAVデータ送信ユニットは前記複数認証デジタルAVデータ受信ユニットの各機能を有することを特徴とする請求項14記載のデジタルAVデータ送受信システムである。

## 【0026】

また請求項16の本発明は前記複数認証デジタルAVデータ受信ユニットの各機能を有するデジタルAVデータ送信ユニット、あるいは前記デジタルAVデータ送信ユニットの機能を有する複数認証デジタルAVデータ受信ユニットが二つ以上互いに接続され、且つ、前記単一認証デジタルAVデータ受信ユニットが二つ以上接続され、デジタルAVデータを互いにやりとりできることを特徴とする請求項15記載のデジタルAVデータ送受信システムである。

## 【0027】

また、請求項17の本発明は、請求項1～16のいずれかに記載のユニット又はシステムが有する各構成要素が持つ機能の全部又は一部を実現するためのプログラムを格納したことを特徴とする媒体である。

## 【0028】

## 【発明の実施の形態】

以下に本発明の実施の形態を図面を参照して説明する。

## 【0029】

まず、第一の実施の形態について図1を参照して説明する。

## 【0030】

デジタルAVデータ送信ユニットSTB1は、データ重要性判定手段3、暗号化手段4、送信側複数認証ルール格納手段5、送信側認証選択手段6、送信側認証手段7及びデジタルインターフェースD-I/F8を持つ。このデータ重要性判定手段3は、データ2の重要性を重要度に応じて複数種類に場合分けを行う手段である。このデータの重要度はCGMSで表現されている。このCGMSは放送局から送られてくるデータの内部あるいはヘッダーに存在している。暗号化手段4は、データ2を、認証の過程で作成されたワーク鍵Kw16で暗号化する手

段である。ワーク鍵 Kw 16 を生成するその認証方法は後述する。送信側複数認証ルール格納手段 5 は、複数種類の認証ルールを持つ手段である。例えば、公開鍵と秘密鍵を用いた認証ルールと、共通鍵を用いた認証ルールの 2 種類の認証ルールである。ここでは、公開鍵及び秘密鍵を用いた認証ルールと共通鍵を用いた認証ルールが格納されているとして説明を進める。送信側認証選択手段 6 は、送信側複数認証ルール格納手段 5 が持つ複数種類の認証ルールから一種類の認証ルールを選択する手段である。この際、データ重要性判定手段 3 の判定の結果を参考にする。本実施の形態では、前記の重要度が高いか低いかにより、時間はかかるが偽造や改竄に強い認証ルールとして、公開鍵と秘密鍵を用いた認証ルールを選択し、時間はかからないが、偽造や改竄に弱いルールとして、共通鍵を用いた認証ルールを選択する。送信側認証手段 7 は、選択された認証ルールで実際にデジタル AV データ受信ユニット TV 9 と認証をかわす手段である。デジタルインターフェース D-I/F 8 は、デジタル AV データ受信ユニット TV 9 と AV データや信号のやりとりを行う手段である。

【0031】

デジタル AV データ受信ユニット TV 9 は、デジタルインターフェース D-I/F 10、復号化手段 11、認証要求手段 12、受信側認証手段 13、受信側複数認証ルール格納手段 14、受信側認証選択手段 15 を持つ。この認証要求手段 12 は、デジタル AV データ送信ユニット STB 1 に認証要求を出す手段である。また、受信側複数認証ルール格納手段 14 は、送信側複数認証ルール格納手段 5 に格納された複数の認証ルールと同じ複数の種類の認証ルールを持つ手段である。従って本実施の形態の場合、公開鍵及び秘密鍵を用いた認証ルールと共通鍵を用いた認証ルールを持つ。受信側認証選択手段 15 は上述した受信側複数認証ルール格納手段 14 から、送信側認証選択手段 6 で選択された認証ルールと同じ認証ルールを選択する手段である。受信側認証手段 13 は、その選択された認証ルールで、つまりデジタル AV データ送信ユニット STB 1 で選択された認証ルールを用いて実際にデジタル AV データ送信ユニット STB 1 と認証を互いに交わす手段である。復号化手段 11 はデジタル AV データ送信ユニット STB 1 で暗号化され送信されてきたデジタル AV データをワーク鍵 Kw 17 を用いて復号

化する手段である。ワーク鍵Kw17は前記受信側認証過程で生成されるもので、その生成する方法は前記ワーク鍵Kw16を生成する方法とともに後述する。デジタルインターフェースD-I/F10は、送信ユニットSTB1とAVデータや信号のやりとりを行う手段である。

#### 【0032】

次に、このような本実施の形態の動作を説明する。

#### 【0033】

まず、デジタルAVデータ受信ユニットTV9を構成する、認証要求手段12が、デジタルインターフェースD-I/F10を介して、デジタルAVデータ送信ユニットSTB1に自らのIDを含めて認証要求を出す。もちろんAVデータの送信要求も出す。デジタルAVデータ送信ユニットSTB1は、デジタルインターフェースD-I/F8を介して、前記認証要求を受信する。そうするとデジタルAVデータ送信ユニットSTB1は、まずデータ重要性判定手段3で、これから送信すべきAVデータ2の重要性を判定し場合分けする。すなわちCGMSの値が11なら重要度は高く、そのデータは表示のみ可能であり、コピーすることは禁止される。また、CGMSの値が10の場合は一回のみコピー可能であり、比較的重要なデータである。またCGMSが00の場合は自由に視聴ないしはコピーして使用してよいので、重要でないデータと言える。またCGMSが01となるAVデータは存在しない。このCGMSの値によりデータの重要度の場合分けがなされる。この結果は送信側認証選択手段6に送られ、送信側複数認証ルール格納手段5から最適な認証ルールが選択される。すなわち、最新の映画など重要なデータの場合には、時間がかかるが、偽造や改竄に強い、公開鍵と秘密鍵を用いる認証ルールが選択される。また、ニュースのような重要でないデータの場合には、時間はかからないが、偽造や改竄に弱い、共通鍵を用いる認証ルールが選択される。更にその選択情報は、送信側認証手段7に送られ、デジタルインターフェースD-I/F8を介して、デジタルAV受信ユニットTV9に送られる。デジタルAV受信ユニットTV9においては、受信側認証選択手段15が、その選択情報を利用して受信側複数認証ルール格納手段14から、デジタルAVデータ送信ユニットSTB1で選択された認証ルールと同じ認証ルールを選択す

る。従って選択されている認証ルールは送信側と受信側とで同じになる。そこで、受信側認証手段13と送信側認証手段7とは互いに、デジタルインタフェースD-I/F10およびデジタルインタフェースD-I/F8を介して、認証を行う。認証が成功すれば、後述するようにして送信側にワーク鍵Kw16、また受信側にワーク鍵Kw17が生成される。送信すべきデータ2は生成されたワーク鍵Kw16を用いて、暗号化手段4で暗号化される。そのあと、デジタルインターフェースD-I/F8を介して、デジタルAVデータ受信ユニットTV9に暗号化データとして送信される。デジタルインターフェースD-I/F10を介して暗号化されたデータは、ワーク鍵Kw17を用いて、復号化手段11にて復号化され、データ101になる。これはデータ2と同一のデータであり、デジタルAVデータ送信ユニットSTB1から、デジタルAVデータ受信ユニットTV9にデータが送信されたことになる。

【0034】

最後に、デジタルAVデータ受信ユニットTV9は、ディスプレイ装置の画面にそのデータを表示する。このようにして、データの重要性が高い時は、時間はかかるが、偽造や改竄に強い認証手段が用いられ、またデータの重要性が低い時は、時間はかからないが、偽造や改竄に弱い認証ルールが用いられる。

【0035】

次に前述したようにデジタルAVデータ受信ユニットTV9からデジタル送信ユニットSTB1に認証要求が出たときの認証のやりとりを示し、その結果ワーク鍵Kwを生成する実施の形態を図4と図5を参照して説明する。

【0036】

まず、図4に示すごとき、公開鍵と秘密鍵による認証を行う場合である。この場合受信側は秘密鍵Sbと公開鍵Pbを持つ。また送信側は秘密鍵Saと公開鍵Paを持つ。まずステップ1で受信側が乱数Bを発生する。受信側は自己の認識番号であるIDbと乱数Bを自らの秘密鍵Sbで暗号化した暗号文Sb(B)を送信側に送る。送信側は受信側の認識番号IDbから検索して受信側の公開鍵Pbを入手する。ステップ8で入手した公開鍵Pbで暗号文Sb(B)を復号化する。その結果ステップ9のごとく乱数Bが得られる。さらに、送信側は、ステッ

プ10のごとく乱数Aを発生する。乱数AとBは送信側の秘密鍵S<sub>a</sub>で暗号化され暗号文S<sub>a</sub>(A, B)が作成される。送信側は暗号文S<sub>a</sub>(A, B)と自己の認識番号ID<sub>a</sub>を受信側に送信する。受信側は暗号文S<sub>a</sub>(A, B)と送信側の認識番号ID<sub>a</sub>を受け取る。受信側は、送信側の認識番号ID<sub>a</sub>から検索して送信側の公開鍵P<sub>a</sub>を入手し、ステップ2のごとく、P<sub>a</sub>で暗号文S<sub>a</sub>(A, B)を復号化する。ここで、暗号文S<sub>a</sub>(A, B)から受信側にはステップ1で送った乱数Bと全く同一の乱数Bが得られ、偽造や改竄が行われてないことが受信側にわかる。もし前記2つの乱数が異なっていれば、偽造や改竄が行われたことがわかり不正な相手がいることがわかる。但し、この場合は、公開鍵P<sub>a</sub>, P<sub>b</sub>は正当な者にしか入手できないようになっているものとする。次に受信側はステップ3のごとく、受信側の秘密鍵S<sub>b</sub>で乱数Aを暗号化し、暗号文S<sub>b</sub>(A)を作成する。S<sub>b</sub>(A)は送信側に送られ、ステップ11のごとく既に送信側で持っている、受信側の公開鍵P<sub>b</sub>で暗号文S<sub>b</sub>(A)を復号化する。ステップ10で発生した、乱数Bとステップ11で復号化した乱数Bは全く同一であれば、偽造や改竄が行われていないことが送信側にわかる。もし前記2つの乱数が異なっていれば、偽造や改竄が行われたことがわかり不正な相手がいることがわかる。

【0037】

今、受信側と送信側でやりとりした乱数AとBは偽造や改竄が行われていないとすると、受信側と送信側以外の第3者には乱数AとBは秘密の乱数である。そこで送信側で、ステップ12のごとく、乱数AとBを用いて鍵K<sub>a b</sub>を作成する。同じくステップ4のごとく受信側で乱数AとBを用いて鍵K<sub>a b</sub>を作成する。前記2つのK<sub>a b</sub>は全く同一のものであり共通鍵となっている。次に送信側でステップ13のごとく鍵K<sub>c</sub>を作成する。これを共通鍵K<sub>a b</sub>で暗号化し、暗号文K<sub>a b</sub>(K<sub>c</sub>)を作成して、受信側に送る。受信側はステップ5のごとく共通鍵K<sub>a b</sub>で暗号文K<sub>a b</sub>(K<sub>c</sub>)を復号化してK<sub>c</sub>を得、その結果、受信側が得た鍵K<sub>c</sub>と送信側にある鍵K<sub>c</sub>は全く同一であり、共通鍵となる。次に送信側でステップ14のごとく鍵K<sub>w</sub>を作成する。鍵K<sub>w</sub>は共通鍵K<sub>c</sub>で暗号化され、暗号文K<sub>c</sub>(K<sub>w</sub>)として、受信側に送られる。受信側では、ステップ6のごとく共通鍵K<sub>c</sub>で暗号文K<sub>c</sub>(K<sub>w</sub>)を復号化し、ステップ7のごとくK<sub>w</sub>を得る。送

信側にある鍵 $K_w$ と受信側にある $K_w$ は全く同一で、共通鍵となっている。以上が公開鍵と秘密鍵による認証の過程で得られたワーク鍵 $K_w$ である。

次に図5に示すとき、共通鍵による認証を行う場合の説明をする。この場合、送信側と受信側は共通鍵 $S$ を持つ。なお、この共通鍵は正当な者にしか与えられていない。まず、受信側でステップ15のごとく2個の乱数 $A_1$ 、 $A_2$ を発生し、共通鍵 $S$ で暗号化し、暗号文 $S(A_1A_2)$ を作成し、送信側へ送る。送信側ではステップ20のごとく共通鍵 $S$ で暗号文 $S(A_1A_2)$ を復号化する。そうすると、ステップ21のごとく乱数 $A_1$ と乱数 $A_2$ が得られる。送信側は乱数 $A_2$ を受信側に送る。受信側はステップ16のごとく2つの乱数 $A_1$ と $A_2$ を持つことになる。ステップ15で発生した乱数 $A_2$ とステップ16で送信側から受け取った乱数 $A_2$ が全く同じであれば、送信側で偽造や改竄が行われていないことがわかる。もし、上記2つの乱数が異なっていれば偽造や改竄が行われたことになり認証は失敗する。次に送信側はステップ22のごとく乱数 $B_1$ と $B_2$ を発生し、暗号化して、暗号文 $S(B_1B_2)$ を受信側に送る。受信側はステップ17のごとく共通鍵 $S$ を用いて暗号文 $S(B_1B_2)$ を復号化する。すると、ステップ18のごとく乱数 $B_1$ と $B_2$ が得られる。受信側は乱数 $B_2$ を送信側に送る。送信側はステップ23のごとく乱数 $B_1$ と $B_2$ を持つことになる。ステップ22で発生した乱数と、ステップ23で受信側から受け取った乱数 $B_2$ が同じであれば、受信側に、偽造や改竄が行われていないことがわかり、認証は成功する。もし、上記2つの乱数が異なっていれば、偽造や改竄が行われたことになり認証は失敗である。

【0038】

ここまでで、認証が成功しているとする、乱数 $A_1$ と乱数 $B_1$ は送信側と受信側以外の第3者には秘密の乱数である。送信側ではステップ24のごとく乱数 $A_1$ と乱数 $B_1$ から鍵 $K_w$ を作成する。一方受信側では、ステップ19のごとく乱数 $A_1$ と乱数 $B_1$ から鍵 $K_w$ を作成する。送信側にある鍵 $K_w$ と受信側にある鍵 $K_w$ は全く同一であり、共通鍵となっている。以上が共通鍵による認証の過程で得られたワーク鍵 $K_w$ である。

【0039】

なお、本発明において、選択する認証ルールの種類は、前記公開鍵及び秘密鍵と共通鍵との2種類に限らず、その他の種類でもよく、更に3種類以上の異なる認証ルールを使用するものであってもよい。

—【0040】—

なお、本実施の形態の変形例として、デジタルAVデータ送信ユニット1はデジタルAV受信ユニット9と同じ機能を有し、また、デジタルAVデータ受信ユニット9はデジタルAV送信ユニット1と同じ機能を有するようになっていてもよい。以後それらのユニットのことを、デジタルAVデータ送受信ユニットと呼ぶ。またそれらの送受信ユニットが3台以上が互いに接続されていてもよい。

【0041】

次に本発明の第二の実施の形態について図6を参照して説明する。

【0042】

本実施の形態では、第一の実施の形態がデータの重要度に応じて認証ルールを変えていたのに対して、デジタルAVデータ受信ユニットVTR45が有する認証ルールの種類によって、認証ルールを選択するところが、相違点である。

【0043】

デジタルAVデータ送信ユニットSTB38は、送信側複数認証ルール格納手段41等を持つ。送信側複数認証ルール格納手段41は、複数種類の認証ルールを持つ手段である。これは第一の実施の形態で説明したごとく、例えば、公開鍵と秘密鍵を用いた認証ルールと、共通鍵を用いた認証ルールである。ここでは、公開鍵及び秘密鍵を用いた認証ルールと共通鍵を用いた認証ルールが格納されているとして説明を進める。ユニット認証ルール情報受信手段42は、デジタルAVデータ受信ユニットVTR45から送られて来た認証ルールに関連する情報を受信する手段である。送信側認証取り出し手段53は、その認証ルールに関連する情報に基づいて、送信側複数認証ルール格納手段41から所定の認証ルールを取り出し、送信側認証手段43に渡す手段である。送信側認証手段43は、デジタルAV受信ユニットVTR45と互いに認証を交わす手段である。暗号化手段40は、第一の実施の形態で説明したごとく、認証を交わした結果生成されたワーク鍵Kw53により、データ39を暗号化する手段である。デジタルインター

フェースD-U/F44は、デジタルAVデータ受信ユニットVTR45とデータや信号のやりとりをする手段である。

【0044】

デジタルAVデータ受信ユニットVTR45は、受信側認証ルール格納手段49等を持つ。この受信側認証ルール格納手段49は、第一の実施の形態で説明した場合とは違って、一種類の認証ルールのみ格納する手段である。例えば、公開鍵と秘密鍵を用いた認証ルール、あるいは共通鍵を用いた認証ルールのような認証ルールがある。ここで、受信側認証ルール格納手段49に格納されている認証ルールはデジタルAVデータ受信ユニットVTR45の装置の性質あるいは重要度によって、あらかじめ決められている。すなわちデータの再利用を予定しないTVなどのユニットには時間はかかるが、偽造や改竄に強い認証ルールが格納されており、またデータのコピーを前提とするVTRのようなユニットには、時間はかからないが、偽造や改竄に弱い認証ルールが格納されている。これによって、AVデータの著作権を守ることができる。本実施の形態では デジタルAVデータ受信ユニットVTR45はVTRであるので、受信側認証ルール格納手段49は共通鍵を持つものとして説明をする。認証ルール情報送信手段50は、デジタルAVデータ受信ユニットVTR45が受信側認証ルール格納手段49に有する共通鍵による認証ルールに関連する情報を送信する手段である。受信側認証手段51は、デジタルAV送信ユニットSTB38と互いに認証を交わす手段である。復号化手段47は、第一の実施の形態で説明したごとく、認証を交わした結果生成されたワーク鍵Kw54により、暗号化されたデータを復号化する手段である。

【0045】

次にこのような本実施の形態の動作を説明する。

【0046】

まず、デジタルAVデータ受信ユニットVTR45を構成する、認証要求手段48がデジタルインターフェースD-I/F46を介して、デジタルAVデータ送信ユニットSTB38に認証要求を出す。デジタルAVデータ送信ユニットSTB38は、デジタルインターフェースD-I/F44を介して、前記認証要求



を受信する。また同時に、認証ルール情報送信手段 50 が、受信側認証ルール格納手段 49 を参照し、格納されている認証ルール、つまり共通鍵による認証ルールに関する情報を取り出す。例えば、その共通鍵による認証ルールを示す識別子を、デジタルインターフェース D-I/F 46 を介して、デジタル AV データ送信ユニット STB 38 に送る。ユニット認証ルール情報受信手段 42 が、デジタル AV データ受信ユニット VTR 45 から送られてきた認証ルールに関する情報、つまり共通鍵による認証ルールの識別子を、デジタルインターフェース D-I/F 44 を介して、受け取る。さらに、この認証ルールの識別子は、送信側認証取り出し手段 53 に渡され、送信側複数認証ルール格納手段 41 から、その認証ルールに関する情報に応じた認証ルール、つまり共通鍵による認証ルールを取り出す。その後、取り出された共通鍵による認証ルールは、送信側認証手段 43 に渡される。その後、送信側認証手段 43 と受信側認証手段 51 は互いに、デジタルインターフェース D-I/F 44 と D-I/F 46 を介して、認証を交わす。認証が成功すれば、その結果、第一の実施の形態で説明したごとく、送信側にワーク鍵 Kw 53、受信側にワーク鍵 Kw 54 が生成される。データ 39 は暗号化手段 40 にてワーク鍵 Kw 53 により暗号化される。暗号化されたデータはデジタルインターフェース D-I/F 44 を介して、デジタル AV 受信ユニット VTR 45 に送られる。デジタルインターフェース D-I/F 46 を介して暗号化されたデータは、復号化手段 47 に送られ、ワーク鍵 Kw 54 を用いて復号化され、データ 52 が得られる。

【0047】

なお、本発明において、送信側の認証ルールの種類は、前記共通鍵に限らず、公開鍵及び秘密鍵、またその他の種類でもよく、更に 3 種類以上の異なる認証ルールを使用するものであってもよい。

【0048】

なお、デジタル AV データ受信ユニットは 2 台あり、その一つは共通鍵による認証ルールのみ有し、他の一つは公開鍵及び秘密鍵のみを有するものであってもよい。さらに 3 台以上のデジタル AV データ受信ユニットであってもよい。

【0049】

次に本発明の第三の実施の形態について図7を参照して説明する。

【0050】

第一の実施の形態がデータの重要度に応じて認証ルールを変えていたのに対し、また、第二の実施の形態がデジタルAVデータ受信ユニットの種類によって認証ルールを変えていたのに対し、本実施の形態では、データの重要度とデジタルAV受信ユニットの種類の両方で認証ルールを決めるところが特徴である。

【0051】

本実施の形態では、デジタルAVデータ送信ユニットSTB56と、複数認証デジタルAVデータ受信ユニットTV65と、単一認証デジタルAVデータ受信ユニットVTR72の三種類のユニットを扱う。デジタルAVデータ送信ユニットSTB56は複数認証デジタルAVデータ受信ユニットTV65と単一認証デジタルAVデータ受信ユニットVTR72にデータを送信するユニットである。複数認証デジタルAVデータ受信ユニットTV65に対しては、デジタルAVデータ送信ユニットSTB56においてデータの重要度により複数種類の認証ルールを選択して、そのデータを送信する。また、単一デジタルAVデータ受信ユニットVTR72は自らの持つ一つの認証ルールを用いてデジタルAVデータ送信ユニットSTB56とで認証を行うユニットである。

【0052】

デジタルAVデータ送信ユニットSTB56は、データ重要性判定手段57を持つ。これは、データ82の重要性を重要度に応じて複数種類の場合分けを行う手段である。この重要度は第一の実施の形態で説明したごとくCGMSで表現されている。このCGMSは放送局から送られてくるデータの内部あるいはヘッダーに存在している。暗号化手段64は、データ82を認証の過程で作成されたワーク鍵Kw64で暗号化する手段である。ワーク鍵Kw16を生成する過程は第一の実施の形態で説明した。送信側複数認証ルール格納手段63は、複数種類の認証ルールを持つ。例えば、公開鍵と秘密鍵を用いた認証ルールや、共通鍵を用いた認証ルールである。ここでは、公開鍵及び秘密鍵を用いた認証ルールと共通鍵を用いた認証ルールが格納されているとして説明を進める。送信側認証選択手段59は、送信側複数認証ルール格納手段63が持つ複数種類の認証ルールから

一種類の認証ルールを選択する手段である。この時、データ重要性判定手段 57 の場合分けの結果を参考にする。第一の実施の形態のごとく、本実施の形態では、前記の重要度が高いか低いかにより、時間はかかるが偽造や改竄に強い認証ルールとして、公開鍵と秘密鍵を用いた認証ルールを選択し、時間はかからないが、偽造や改竄に弱い、共通鍵を用いた認証ルールを選択する。ユニット認証ルール情報受信手段 60 は、デジタル AV データ受信ユニット TV 72 から送られて来た認証ルールに関する情報を受信する手段である。送信側認証ルール取り出し手段 58 は、認証ルールに関連する情報に基づいて、送信側複数認証ルール格納手段 63 から所定の認証ルールを取り出し、送信側認証手段 61 に渡す手段である。送信側認証手段 61 は、実際に複数認証デジタル AV データ受信ユニット TV 65 及び単一認証デジタル AV データ受信ユニット VTR 72 と認証を交わす手段である。デジタルインターフェース D-I/F 62 は、複数認証デジタル AV データ受信ユニット TV 65 や単一認証デジタル AV データ受信ユニット VTR 72 と AV データや信号をやりとりする手段である。

#### 【0053】

複数認証デジタル AV データ受信ユニット TV 65 は、認証要求手段 67 を持つ。これは、デジタル AV データ送信ユニット STB 56 に認証要求を出す手段である。また、受信側複数認証ルール格納手段 68 は、送信側複数認証ルール格納手段 63 と同じ複数種類の認証ルールを持つ。従って本実施の形態の場合、公開鍵及び秘密鍵を用いた認証ルールと共通鍵を用いた認証ルールがある。受信側認証選択手段 69 は、受信側複数認証ルール格納手段 68 から、送信側認証選択手段 59 で選択された認証ルールと同じ認証ルールを選択する手段である。受信側認証手段 70 は、その選択された認証ルールで、つまりデジタル AV データ送信ユニット STB 56 で選択された認証ルールを用いて実際にデジタル AV データ送信ユニット STB 56 と認証を互いに交わす手段である。復号化手段 66 は、デジタル AV データ送信ユニット STB 56 で暗号化されたデジタル AV データをワーク鍵 Kw 80 を用いて復号化する手段である。ワーク鍵 Kw 80 は前記認証過程で生成されるもので、その生成する方法は前記ワーク鍵 Kw 79 とともに第一の実施の形態で説明した。デジタルインターフェース D-I/F 71 は、

デジタルAVデータ送信ユニットSTB56とAVデータや信号のやりとりを行う手段である。

【0054】

単一認証デジタルAVデータ受信ユニットVTR72は、受信側認証ルール格納手段75を持つ。これは、前述したごとく一種類の認証ルールのみ格納する手段である。例えば、公開鍵と秘密鍵を用いた認証ルール、あるいは共通鍵を用いた認証ルールのような認証ルールがある。ここで、受信側認証ルール格納手段75に格納されている認証ルールは単一認証デジタルAVデータ受信ユニットVTR72の装置の種類や、重要度によって、あらかじめ決められている。ここでは、受信側認証ルール格納手段75が共通鍵を持つものとして説明をする。認証ルール情報送信手段76は、単一認証デジタルAVデータ受信ユニットVTR72が受信側認証ルール格納手段75に有する共通鍵による認証ルールに関連する情報を送信する手段である。受信側認証手段77は、デジタルAVデータ送信ユニットと互いに認証を交わす手段である。復号化手段73は、第一の実施の形態で説明したごとく、認証を交わした結果生成されたワーク鍵Kw81により、暗号化されたデータを復号化する手段である。

【0055】

次にこのような本実施の形態の動作を説明する。

【0056】

まず、はじめに複数認証デジタルAVデータ受信ユニットTV65かまたは単一認証デジタルAVデータ受信ユニット72が認証要求を出す。デジタルAVデータ送信ユニットSTB56はどのユニットから認証要求が送られて来たのかを判断する。

【0057】

以下、まず複数認証デジタルAVデータ受信ユニットTV65から認証要求が来た場合を説明し、次に単一認証デジタルAVデータ受信ユニットVTR72から認証要求が来た場合の説明を行う。

【0058】

第一に、前述したように複数認証デジタルAVデータ受信ユニットTV65を

構成する、認証要求手段 67 が、デジタルインターフェース D-I/F 71 を介して、デジタル AV データ送信ユニット STB 56 に自らの ID を含めて認証要求を出す。デジタル AV データ送信ユニット STB 56 は、デジタルインターフェース D-I/F 62 を介して、前記認証要求を受信する。そうするとデジタル AV データ送信ユニット STB 56 は、まずデータ重要性判定手段 57 で、これから送信すべきデータ 82 の重要性を判定し場合分けする。この結果は送信側認証選択手段 59 に送られ、送信側複数認証ルール格納手段 63 から最適な認証ルールが選択される。すなわち、重要なデータの場合には、公開鍵と秘密鍵を用いる認証ルールが選択される。また、重要でないデータの場合には、共通鍵を用いる認証ルールが選択される。更にその選択情報は、送信側認証手段 61 に送られ、デジタルインターフェース D-I/F 62 を介して、複数認証デジタル AV データ受信ユニットに送られる。複数認証デジタル AV データ受信ユニットにおいては、受信側認証選択手段 69 が、その選択情報を利用して受信側複数認証ルール格納手段 68 からデジタル AV データ送信ユニット STB 56 で選択された認証ルールと同じ認証ルールを選択する。従って選択されている認証ルールは送信側と受信側とで同じになる。受信側認証手段 70 と送信側認証手段 61 とは互いに、デジタルインターフェース D-I/F 71 およびデジタルインターフェース D-I/F 62 を介して、認証を行う。認証が成功すれば、第一の実施の形態で詳述したごとく、送信側にワーク鍵 Kw 79、また受信側にワーク鍵 Kw 80 が生成される。送信すべきデータ 82 は生成されたワーク鍵 Kw 79 を用いて、暗号化手段 64 で暗号化される。そのあと、デジタルインターフェース D-I/F 62 を介して、複数認証デジタル AV データ受信ユニット TV 65 に暗号化されたデータとして送信される。デジタルインターフェース D-I/F 71 を介して暗号化されたデータは、ワーク鍵 Kw 80 を用いて、復号化手段 66 にて復号化され、データ 83 になる。これはデータ 82 と同一のデータであり、デジタル AV データ送信ユニット STB 56 から、複数認証デジタル AV データ受信ユニット TV 65 にデータが送信されたことになる。このようにして、データの重要性が高い時は、時間はかかるが、偽造や改竄に強い認証ルールが用いられ、またデータの重要性が低い時は、時間はかからないが、偽造や改竄に弱い認証ルールが

用いられる。

【0059】

次に単一認証デジタルAVデータ受信ユニットVTR72から認証要求が来た場合の動作の説明を行う。まず、単一認証デジタルAVデータ受信ユニットVTR72を構成する、認証要求手段74がデジタルインターフェースD-I/F78を介して、デジタルAVデータ送信ユニットSTB56に認証要求を出す。デジタルAVデータ送信ユニットSTB56は、デジタルインターフェースD-I/F62を介して、前記認証要求を受信する。同時に認証ルール情報送信手段76が、受信側認証ルール格納手段75を参照し、格納されている認証ルール、つまり共通鍵による認証ルールに関する情報を取り出す。例えば、その共通鍵による認証ルールを示す識別子を、デジタルインターフェースD-I/F78を介して、デジタルAVデータ送信ユニットSTB56に送る。ユニット認証ルール情報受信手段60が、単一認証デジタルAVデータ受信ユニットVTR72から送られてきた認証ルールに関する情報、つまり共通鍵による認証ルールの識別子を、デジタルインターフェースD-I/F62を介して、受け取る。さらにこの認証ルールの識別子は、送信側認証ルール取り出し手段58に渡され、送信側複数認証ルール格納手段63から、その認証ルールに関する情報に応じた認証ルール、つまり共通鍵による認証ルールは、送信側認証手段61に渡される。送信側認証手段61と受信側認証手段77は互いに、デジタルインターフェースD-I/F62とD-I/F78を介して、認証を交わす。認証が成功すれば、その結果、第一の実施の形態で詳述したごとく、送信側にワーク鍵Kw79、受信側にワーク鍵Kw81が生成される。認証の結果ワーク鍵が生成される過程は、第一の実施の形態で詳述した。データ82は暗号化手段64にてワーク鍵Kw79により暗号化される。暗号化されたデータはデジタルインターフェースD-I/F62を介して、単一認証デジタルAVデータ受信ユニットVTR72に送られる。デジタルインターフェースD-I/F78を介して暗号化されたデータは、復号化手段Kw81に送られ、ワーク鍵Kw81を用いて復号化され、データ84が得られる。これはデータ82と同一のデータであり、デジタルAVデータ送信ユニットSTB56から、単一認証デジタルAVデータ受信ユニットVTR72に

データが送信されたことになる。

【0060】

次に、本発明の第四の実施の形態を説明する。

【0061】

本実施の形態では、デジタルAVデータ受信ユニットが正当なものか不正なものを調べて作成しておいた管理基準（CRL）を利用するものである。そのCRLの作成の仕方は、例えば、消費者が購入した販売店が発行した登録カードを元に作成する方法等が考えられる。

【0062】

図8は、その管理基準を放送局から送られてくるデジタルAVデータの重要度に応じて、その管理基準を参照するかどうか決定するものである。

【0063】

デジタルAV送信ユニットSTB93は、放送局から送られてくるデジタルAVデータの重要度に応じて、データの重要性を判定する、データ重要性判定手段86を有する。また、データの重要度に応じて管理基準格納手段88に格納されている管理基準情報（CRL）を参照するかどうかを判定する、管理基準参照決定手段87を有する。また、前記決定結果に従って、認証を行うかどうかを決定する、認証決定手段89を有する。また、実際にデジタルAVデータ受信ユニットTV92と認証を交わす、認証手段90を有する。前記認証手段90は、デジタルインターフェースD-I/F91を介して、デジタルAVデータ受信ユニットTV92に接続している。

【0064】

次に本実施の形態の動作を説明する。まず、放送局から送られてくるデジタルAVデータ85は、データ重要性判定手段86で、重要性を判定される。その結果は、管理基準参照決定手段87に渡され、管理基準格納手段88に格納されている情報を参照すべきかどうか決定される。例えば、新作の映画等の場合は重要なので、管理基準情報を参照すると決定する。また、ニュース等の場合は重要でないなので、管理基準情報を参照しないと決定する。さらに認証決定手段89で、前記管理基準参照決定手段87の判定決定に従って、認証すべきかどうか決定さ

れる。すなわち、デジタルAVデータ受信ユニットTV92が、デジタルAVデータ85を受信するのに正当な機器か不当な機器かを、管理基準格納手段88に格納されている管理基準情報で判断される。正当であると判断されれば、次の認証手段90で、デジタルインターフェースD-I/F91を介して、デジタルAV受信ユニットTV92と認証が交わされる。不当と判断されればその時点で、デジタルAVデータ受信ユニットとの認証は交わされず、データ85の送信はされない。

【0065】

他方、図9は上述した管理基準を、デジタルAVデータ受信ユニットの装置の種類、あるいは重要度に応じて、その管理基準を参照するかどうか決定するものである。

【0066】

デジタルAVデータ送信ユニットSTB94は、デジタルAVデータ受信ユニット100の装置の種類あるいは、重要度に応じて、その管理基準格納手段96を参照すべきかどうかを決定する、管理基準参照決定手段95を有する。また、認証決定手段97は、認証するかどうかを決定する。管理基準格納手段96は、デジタルAV受信ユニット100がデジタルAVデータを受信するのに正当な機器か正当でない機器かの情報が格納されている。認証手段98は、デジタルインターフェースD-I/F99を介して、デジタルAVデータ受信ユニットVTR100と認証を行う。

【0067】

次に本実施の形態の動作を説明する。まず、デジタルAVデータ受信ユニットVTR100が、デジタルインターフェースD-I/F99を介して、管理基準参照決定手段95に機器情報を送る。これを受けて、管理基準参照決定手段95は、管理基準格納手段96に格納されている情報を参照すべきかどうかを決定する。管理基準格納手段96を参照すると決定された場合は、認証決定手段97は、まず、管理基準格納手段96を参照して、デジタルAVデータ受信ユニットがデータを受信するのに正当な機器か、不正な機器かを判定する。ここで、正当な機器と判定されれば、次の認証手段98にて、デジタルインターフェースD-I



／F99を介して、デジタルAVデータ受信ユニットと認証を開始する。デジタルAVデータ受信ユニットがデータを受信するのに不正な機器と判定された場合は、認証は行われず、データの送信も行われない。

【0068】

なお、STBを送信ユニットとして説明してきたが、VTRで録画したデータを再生する際には、前記VTRが送信ユニットとなる。この際CGMSが入力時「1回コピー可」であれば「コピー不可」に書き換えられて出力される。ここで、データの重要度としては、元の入力時における重要度と考えるべきであり、「1回コピー可」と同様の認証ルールを使うこともできる。このように「1回コピーの結果コピー不可となったデータ」と「元からコピー不可のデータ」を見分ける必要がある際には、前述した、存在しないCGMS値01を前者の区別用に割り当てることもできる。

【0069】

さらに、本発明の各構成要素は、それぞれの機能を実現する専用のハード回路、機器等で実現しても、あるいは、コンピュータを利用してソフトウェア的に実現してもかまわない。

【0070】

さらに、本発明をコンピュータで実現する場合、それらの各構成要素の機能の全部又は一部を実現するためのプログラムを格納した媒体も本発明に属する。

【0071】

【発明の効果】

以上説明したところから明らかなように、本発明は、重要でないデータの認証に多くの時間を要せず、重要なデータに関しては、その認証が偽造や改竄に強くまた、ユニットによって認証に必要な厳密さを変えることによって、データの重要性や相手の装置が有する認証方法の種別などを考慮して、適切な認証方法でデータの送受信を行いうるユニット、システム等を提供することができる。

【図面の簡単な説明】

【図1】

本発明の第一の実施の形態についての概略図

【図 2】

従来技術について示す概略図

【図 3】

従来技術について示す概略図

【図 4】

本発明の実施の形態のうち認証方法に関するブロック図

【図 5】

本発明の実施の形態のうち認証方法に関するブロック図

【図 6】

本発明の第二の実施の形態についての概略図

【図 7】

本発明の第三の実施の形態についての概略図

【図 8】

本発明の第四の実施の形態についての概略図

【図 9】

本発明の第四の実施の形態についての概略図

【符号の説明】

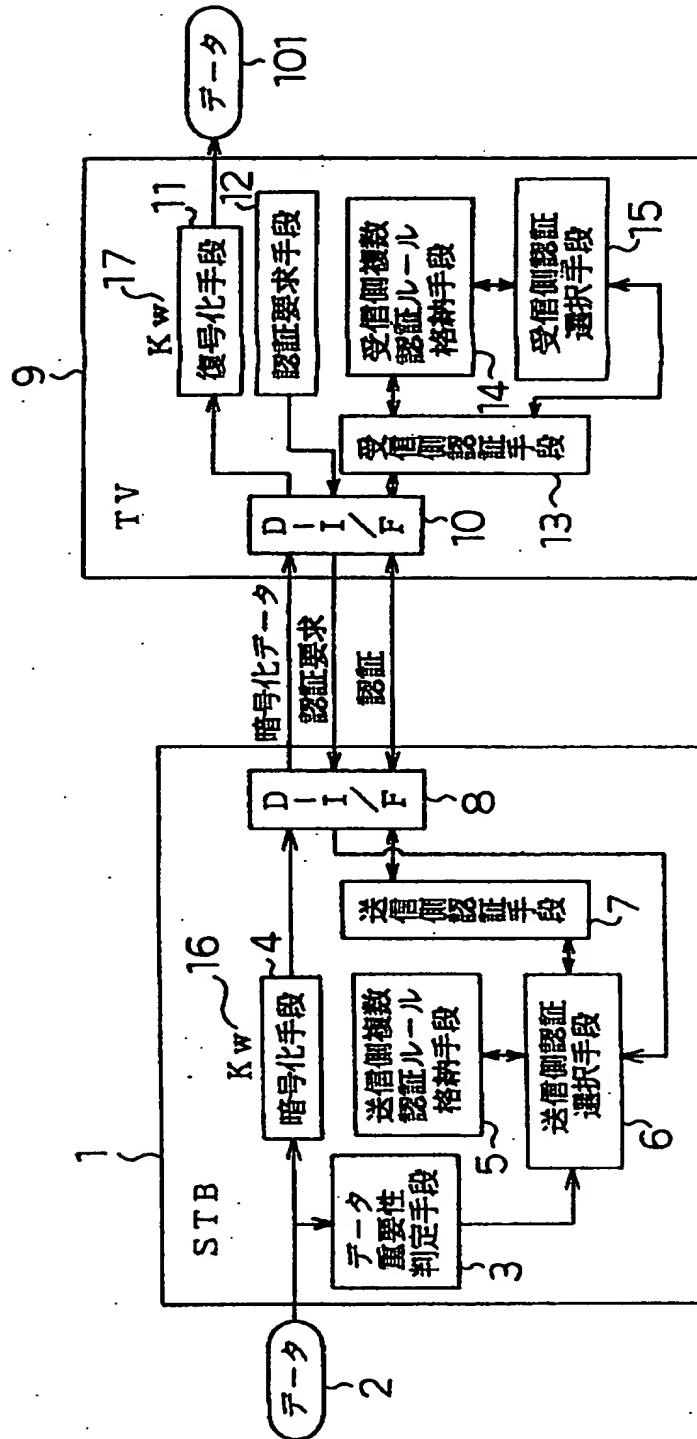
- 1 STB
- 3 データ重要性判定手段
- 5 送信側複数認証ルール格納手段
- 6 送信側認証選択手段
- 7 送信側認証手段
- 9 TV
- 13 受信側認証手段
- 14 受信側複数認証ルール格納手段
- 15 受信側認証選択手段
- 18 STB
- 19 認証手段
- 20 公開鍵／秘密鍵

- 23 TV
- 25 認証手段
- 26 公開鍵／秘密鍵
- 28 STB
- 29 認証手段
- 30 共通鍵
- 33 TV
- 35 認証手段
- 36 共通鍵
- 38 STB
- 41 送信側複数認証ルール格納手段
- 42 ユニット認証ルール情報受信手段
- 43 送信側認証手段
- 45 VTR
- 48 認証要求手段
- 49 受信側認証ルール格納手段
- 50 認証ルール情報送信手段
- 51 受信側認証手段
- 55 送信側認証ルール取り出し手段
- 56 STB
- 57 データ重要性判定手段
- 58 送信側認証ルール取り出し手段
- 59 送信側認証選択手段
- 60 ユニット認証ルール情報受信手段
- 61 送信側認証手段
- 63 送信側複数認証ルール格納手段
- 65 TV
- 67 認証要求手段
- 68 受信側複数認証ルール格納手段

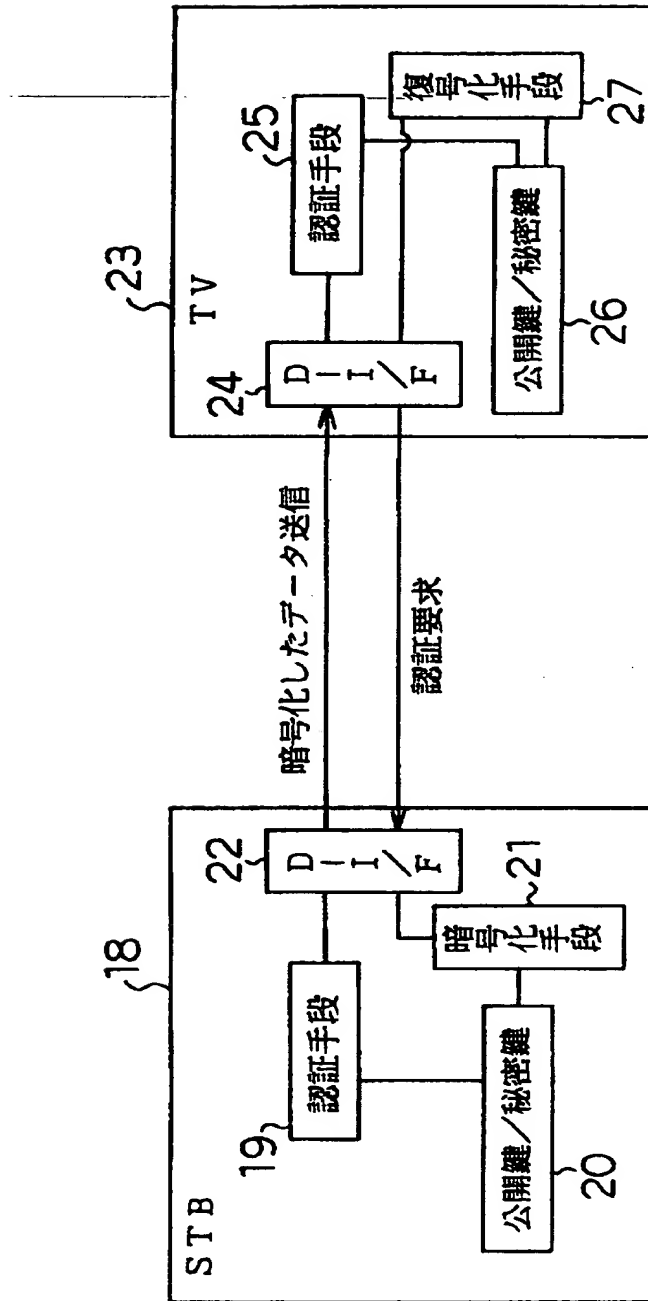
69	受信側認証選択手段
70	受信側認証手段
72	VTR
74	認証要求手段
75	受信側認証ルール格納手段
76	認証ルール情報送信手段
77	受信側認証手段
86	データ重要性判定手段
87	管理基準参照決定手段
88	管理基準格納手段
89	認証決定手段
90	認証手段
92	TV
93	STB
94	STB
95	管理基準参照決定手段
96	管理基準格納手段
97	認証決定手段
98	認証手段
100	VTR

【書類名】 図面

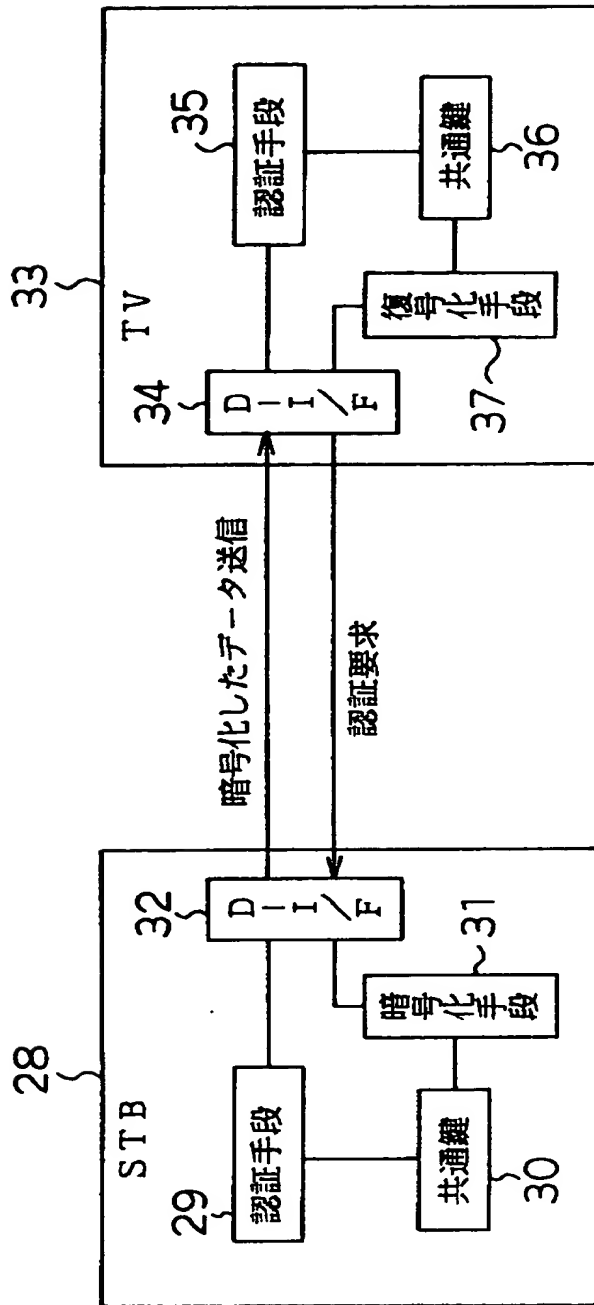
【図 1】



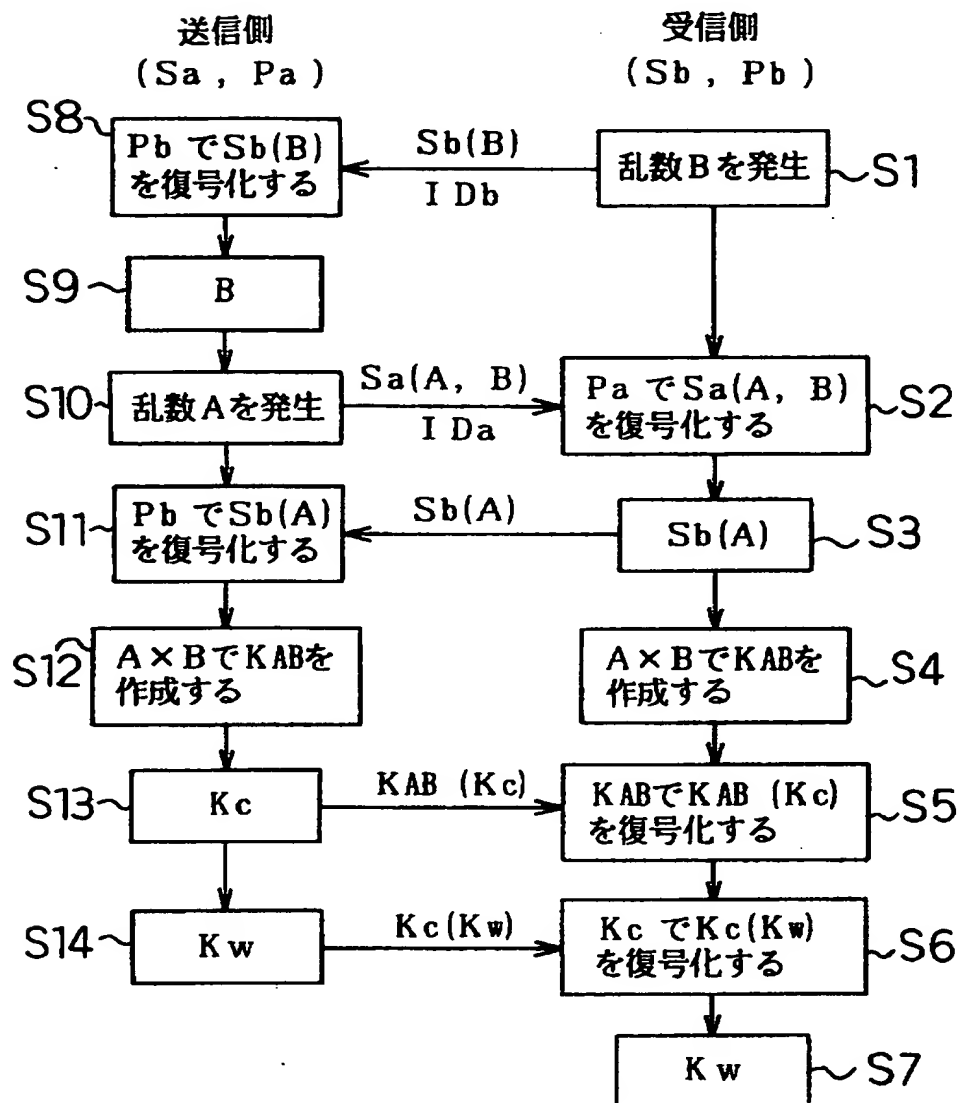
【図 2】



【図 3】

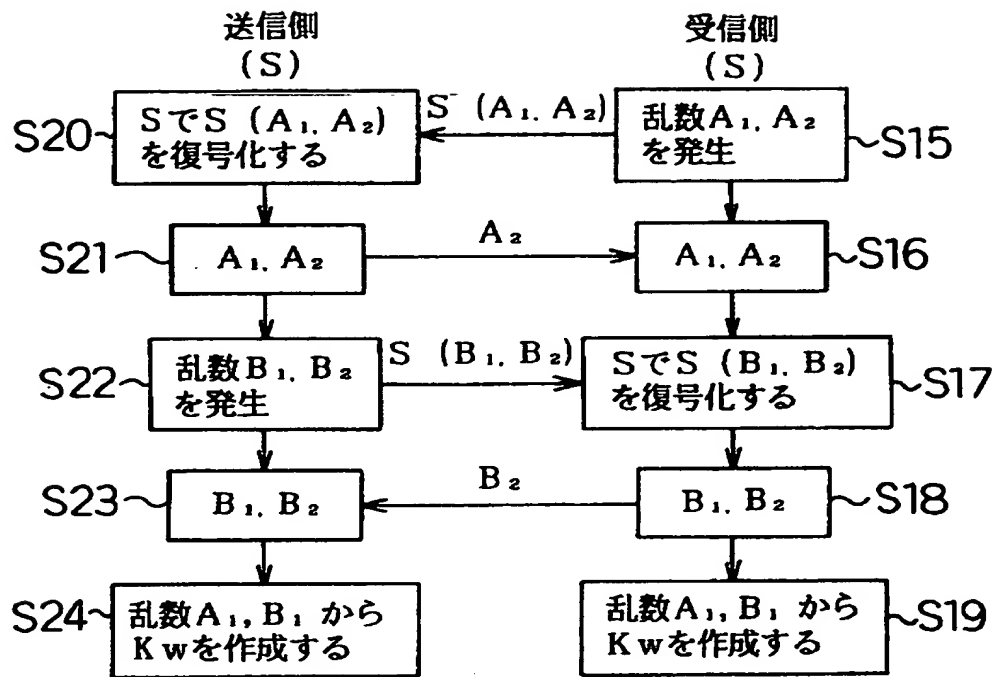


【図 4】

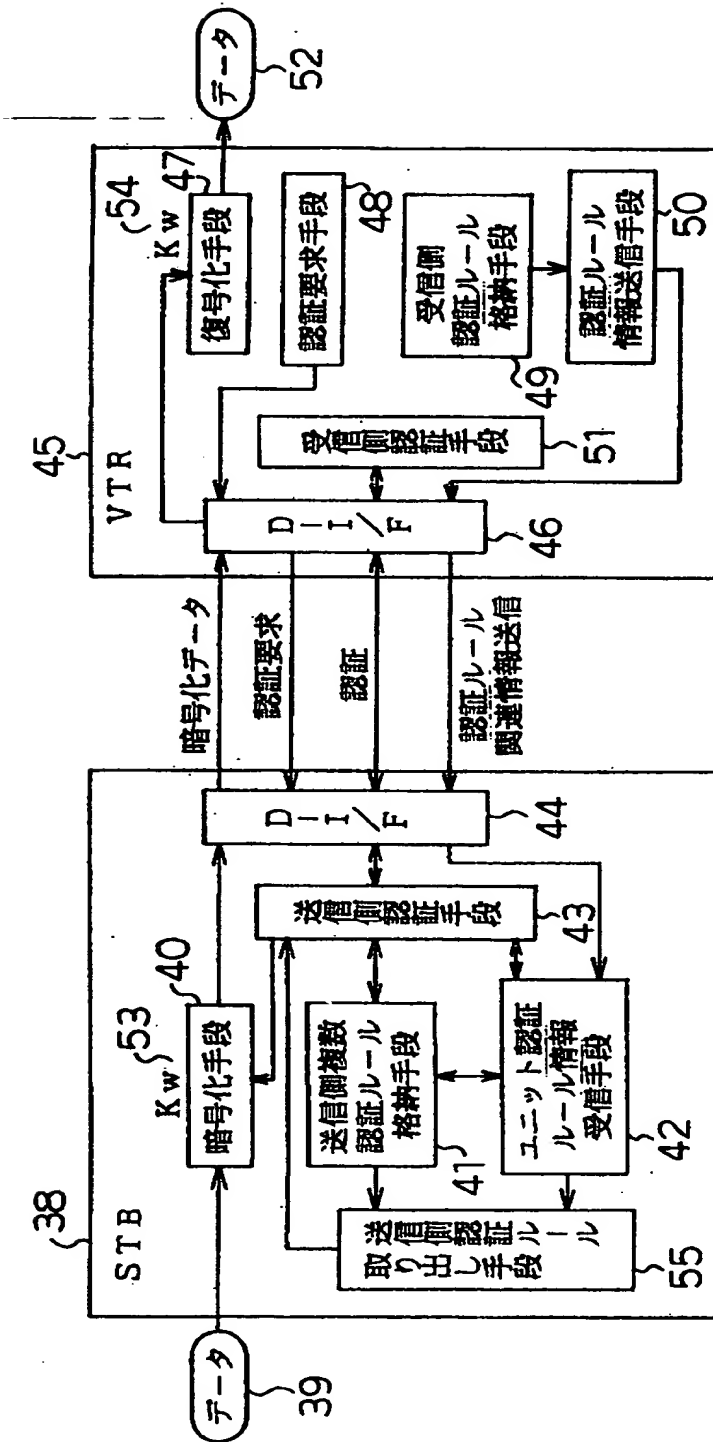




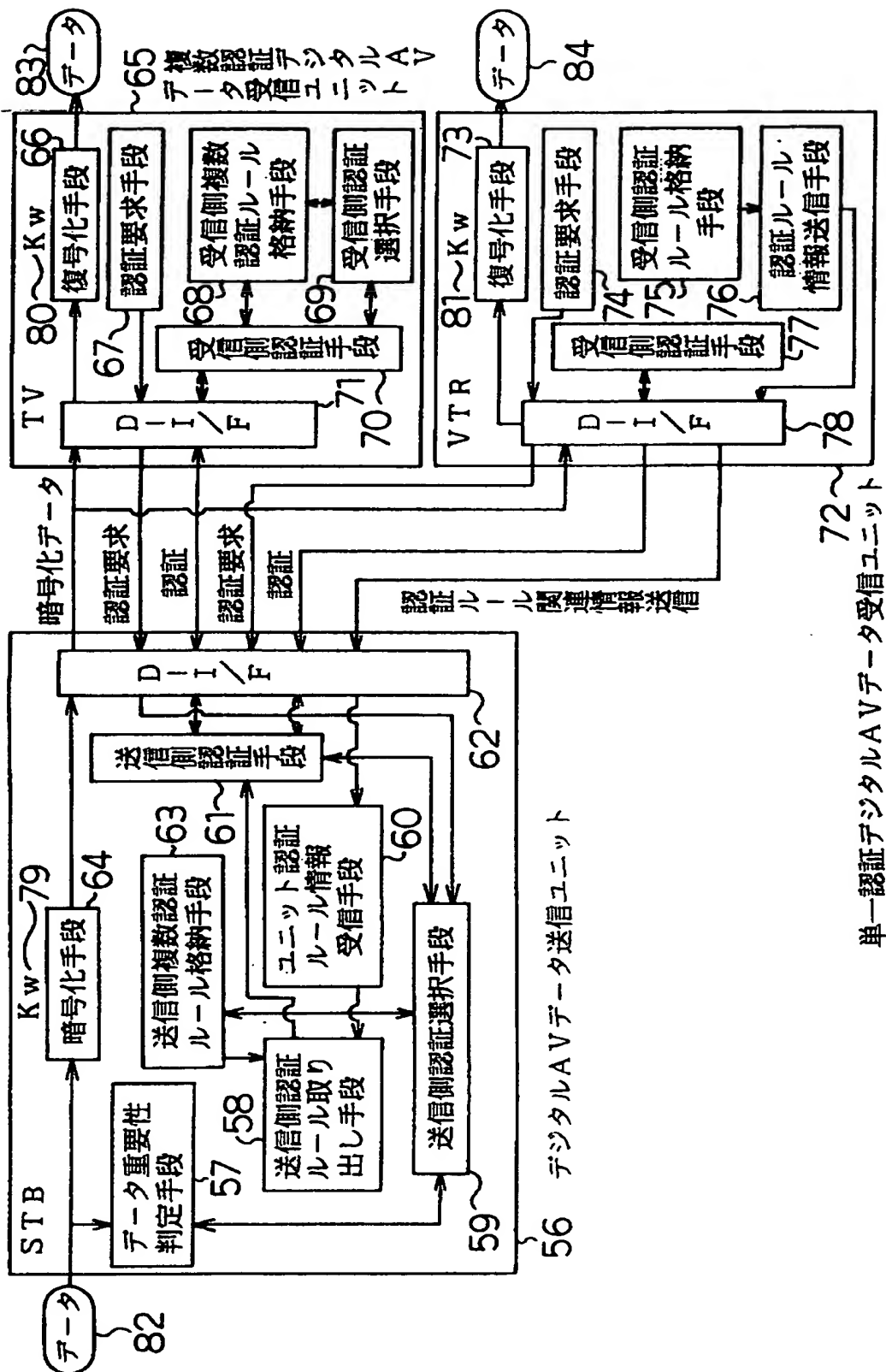
【図 5】



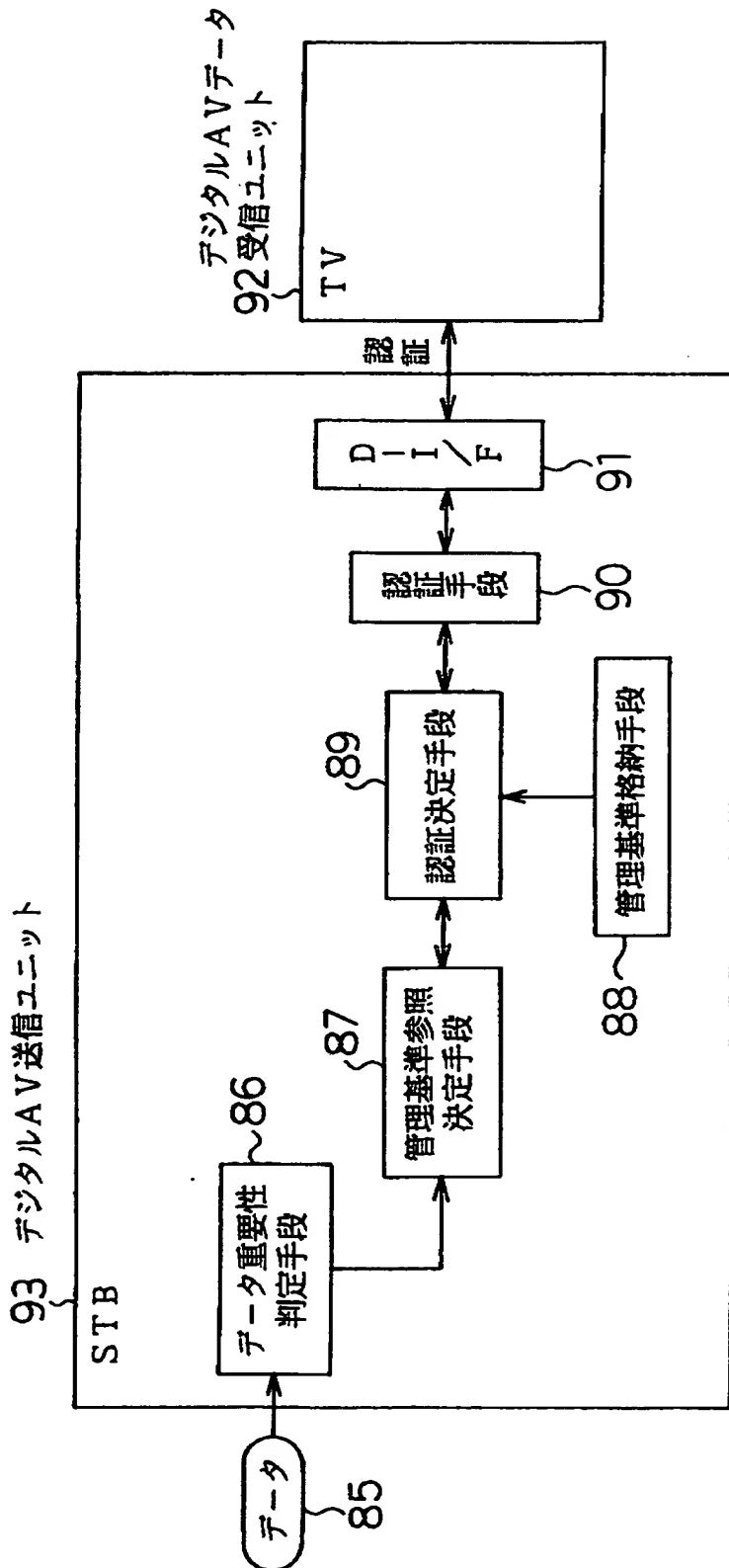
【図 6】



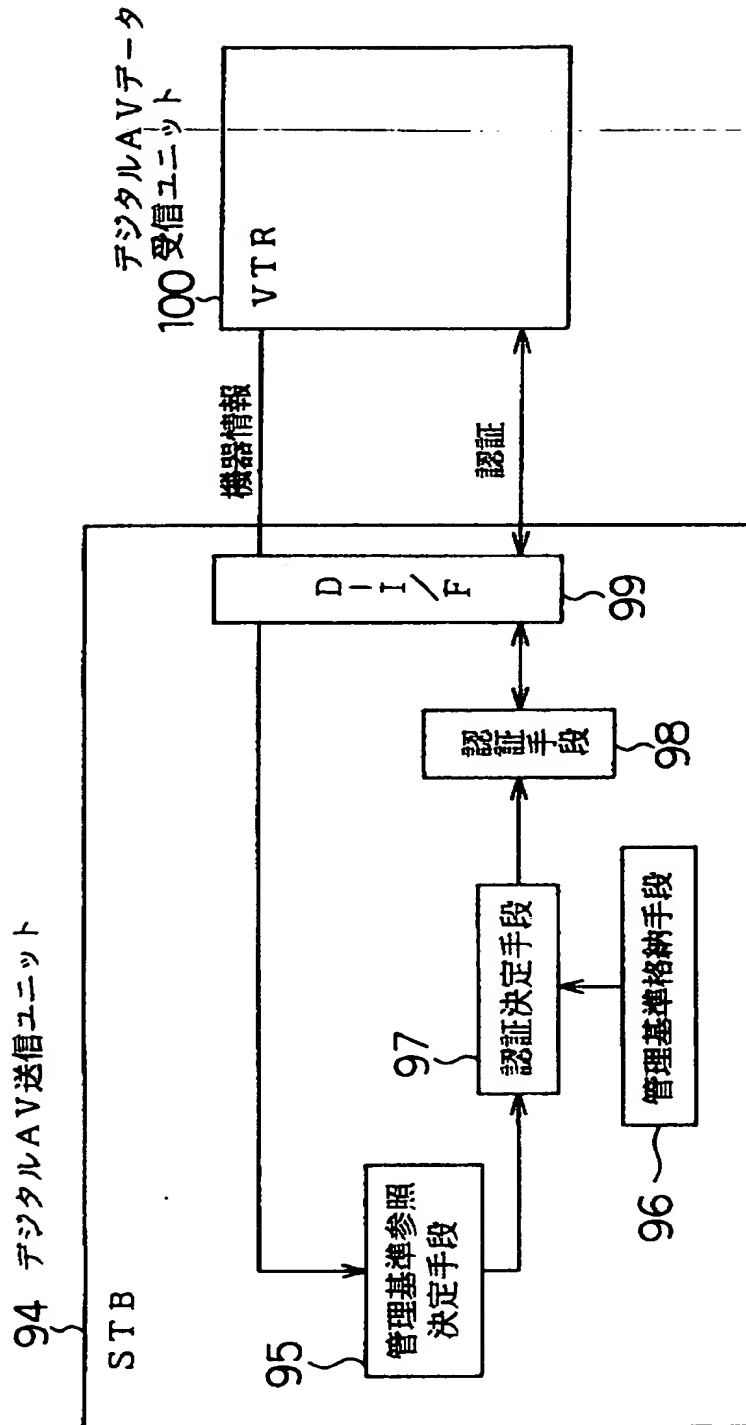
【図7】



【図 8】



【図9】



【書類名】 要約書

【要約】

【課題】 従来AVデータ装置間のデータの通信では、重要でないデータの認証に多くの時間を要したり、重要なデータであってもその認証が偽造や改竄に弱いという課題がある。

【解決手段】 デジタルAVデータの重要度を判定する判定手段3と、複数種類の認証ルールを格納したルール格納手段5と、認証要求を受け、判定手段3の判定結果に基き、ルール格納手段5から一種類のルールを選択する認証選択手段6と、その選択された認証ルールに基づいて認証を行う認証手段7とを有するデジタルAV送信ユニットSTB1と、認証の要求を行う認証要求手段12と、ルール格納手段5と同じ複数種類の認証ルールを格納したルール格納手段14と、認証選択手段6で選択された所定の認証ルールと同じ認証ルールを認証ルール格納手段14から選択する証選択手段15と、受信側で選択された認証ルールに基づいて認証を行う認証手段13とを有するデジタルAVデータ受信ユニットTV9とを備えたデジタルAVデータ送受信システム。

【選択図】 図1

【書類名】 職権訂正データ  
【訂正書類】 特許願

<認定情報・付加情報>

——【特許出願人】——

【識別番号】	000005821
【住所又は居所】	大阪府門真市大字門真 1 0 0 6 番地
【氏名又は名称】	松下電器産業株式会社
【代理人】	申請人
【識別番号】	100092794
【住所又は居所】	大阪市淀川区宮原 5 丁目 1 番 3 号 新大阪生島ビル 松田特許事務所
【氏名又は名称】	松田 正道

出願人履歴情報

識別番号

[000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住 所 大阪府門真市大字門真1006番地  
氏 名 松下電器産業株式会社